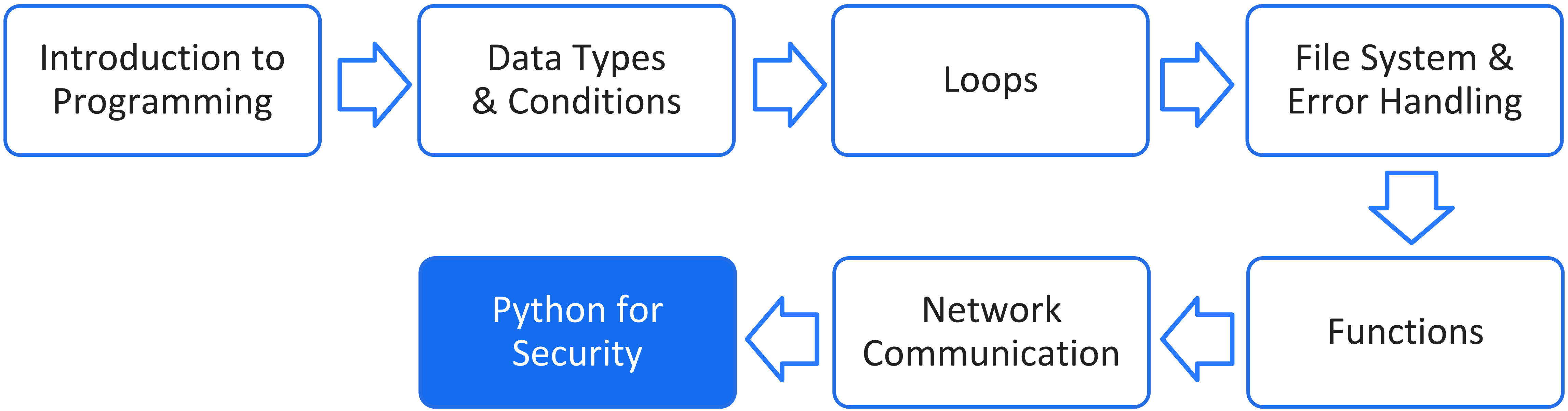
Cybersecurity Professional Program

Python for Security

Introduction to Python for Security

Introduction to Python for Security

Course Path



Introduction to Programming

Data Types & Conditions

Loops

File System & Error Handling

Functions

Network Communication

Python for Security

Objectives

This lesson is a summary of the Introduction to Python module. It focuses on the creation of a fully configured and working script.

- Overview
- Project Requirements
- Project Steps

Python for Security

Overview

Overview

Python for Security

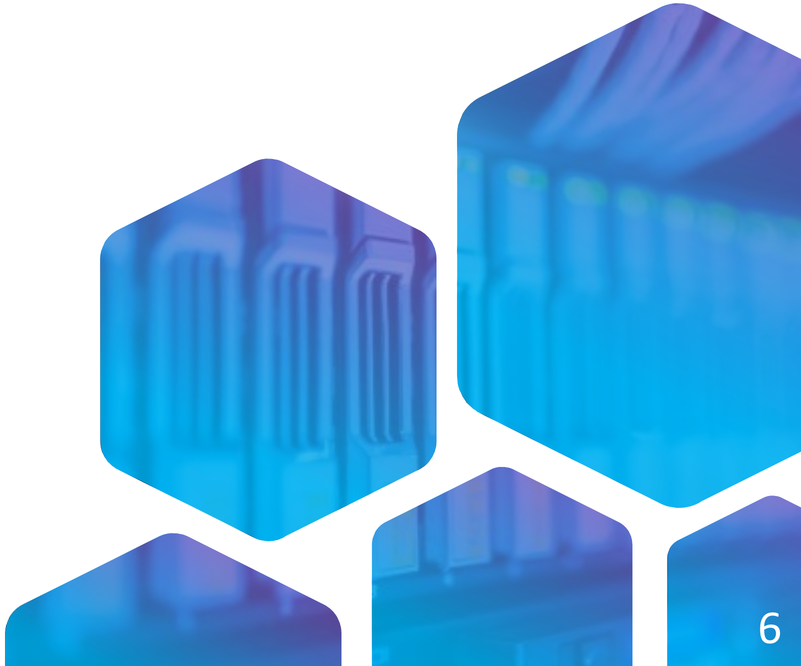
- Can be used for security purposes
- Dedicated libraries are constantly being developed.
- Flexible security measures

Overview

Information Gathering

Critical Information
Identifying the relevant information and knowing how to leverage it

Log Parsing
Extraction of specific information from logs without the use of third parties

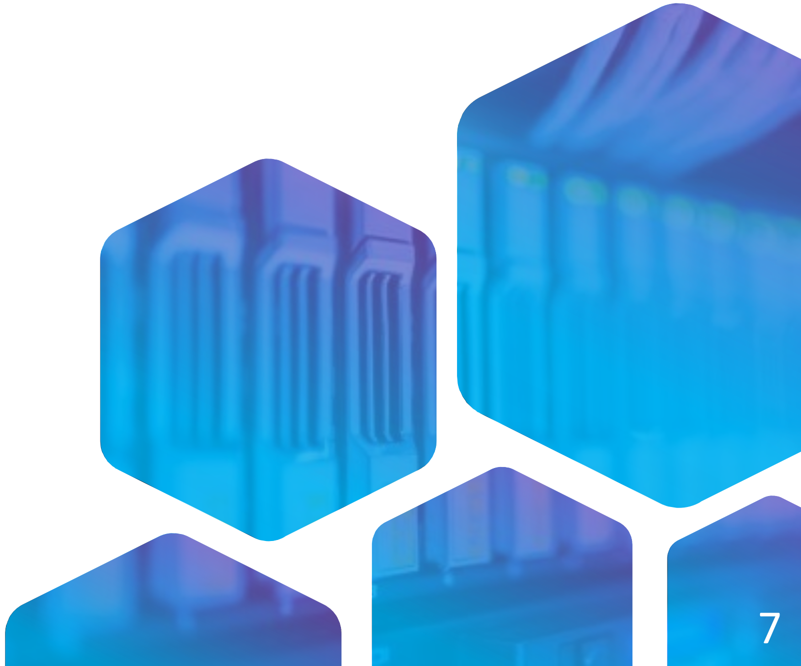


Overview

Forensic Tools

Finding Evidence
Every compromised system or suspicious activity leaves some kind of evidence behind.

Data Analysis
Python can help analyze data, locate evidence faster, and determine conclusions based on the evidence.



Overview

Automation

Efficiency
Performing a procedure with minimal human assistance

SIEM Integration
Used for process automation in SIEM systems

Overview

ARP Spoof

- MAC address impersonation
- Manipulating data in an ARP table
- Commonly used in On-Path attacks
- Identified by MAC address duplication

Overview

ARP Spoof Detector

- Automated detection script
- Identifies if a machine is under attack

The project that follows involves building an ARP Spoof detector.

Python for Security

Project Requirements

Requirements

Before You Start

- Read the story before starting.
- Divide the objective into smaller goals.
- Write a workplan before starting.
- Combine the different goals into a working script.

> It is recommended to verify the output of the code at each and every step.

Requirements

The Story

- The HackRS company suspects an On-Path attack on multiple stations is under way.
- Verify if a station is being ARP Spoofed.
- Use Python to perform the verification.

> The script should check if the current machine is under an On-Path attack via ARP Spoof.

Python for Security

Project Steps

Project Steps

ARP Table Extraction

The ARP table can be accessed via the OS library.

Its lines should be extracted and saved.

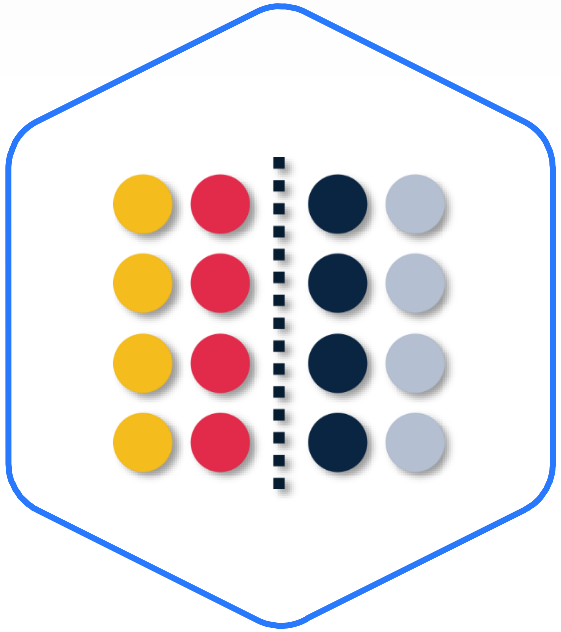
Project Steps

Address Dictionary Creation

Filter the extracted data and save it to a dictionary for easy use.

Project Steps

Duplication Check



Check if a MAC address exists more than once in the system.

If so, a notification should be printed.

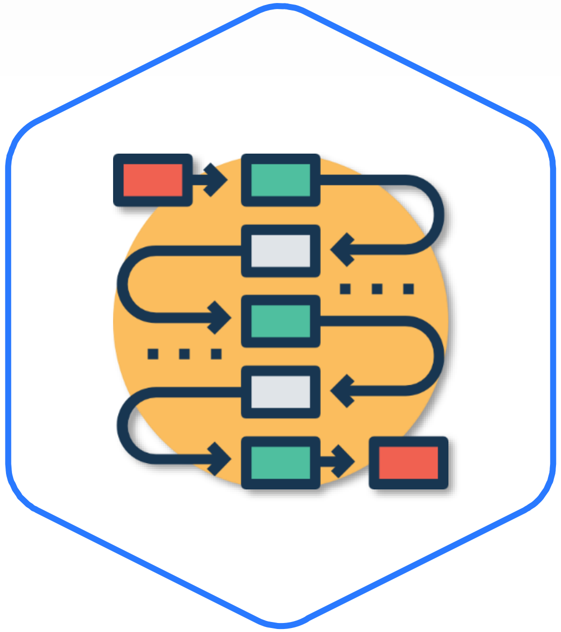
Project Steps

Logging

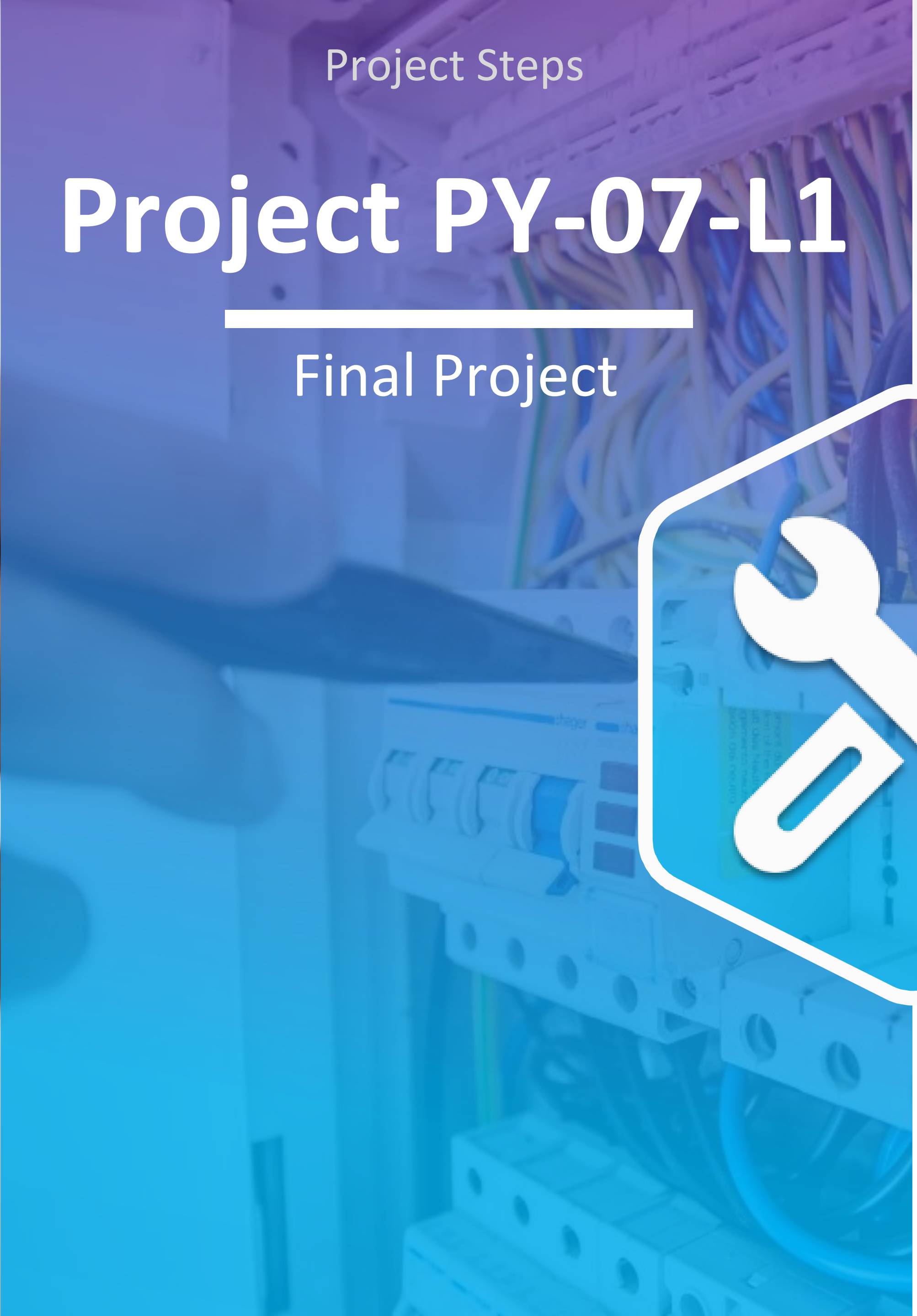
The program must log ARP Spoofing activity by creating a log file that includes time-related data (when the activity occurred, for how long, etc.).

Project Steps

Correct Functionality



- Make sure the program is divided into functions, the variables have logical names, and the program has an overall logical flow.
- The program must be executed only if the main file is run.



Project PY-07-L1

Final Project

Mission

Create a program that can detect active ARP Spoofing attacks on host machines.

Steps

- Extract the ARP table.
- Perform ARP table entry filtration.
- Locate MAC address duplications.
- Generate logs based on attacks.

Environment & Tools

- Kali Linux ISO
- Windows
- PyCharm
- Python 3

Related Files

- Project document

Project Steps

TDX Arena Asynchronous Learning

Shifting Left for Security

Mission

Use TDX Arena to practice secure Python coding.

Steps

- Sign into the **TDX Arena** platform.
- Navigate to the **Practice Arena**.
- Navigate to the **Python Programming** course.
- Select ***PY05 Secure Programming***.
- Select the ***Shifting Left for Security*** lab.

Complete this lab as a learning opportunity.

Project Steps

TDX Arena Asynchronous Learning

Log Analyzer

Mission

> Use TDX Arena to practice everything you have learned to analyze an Apache log.

Steps

- Sign into the **TDX Arena** platform.
- Navigate to the **Practice Arena**.
- Navigate to the **Python Programming** course.
- Select ***PY07 Putting It All Together***.
- Select the ***Log Analyzer*** lab.

Complete this lab as a learning opportunity.

Thank You

Questions?